

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|

# MULTIMEDIA UNIVERSITY

## FINAL EXAMINATION

MASTER OF CS (SOFTWARE ENGINEERING AND SOFTWARE ARCHITECTURE)  
TRIMESTER 1521

### TSC7011 – SECURITY IN COMPUTING

(All sections / Groups)

26 JANUARY 2016  
10.00 am - 01.00 pm  
(3 Hours)

#### INSTRUCTIONS TO STUDENTS

1. This Question paper consists of **ELEVEN** pages (excluding this page) with **FIVE** Questions.
2. Attempt **FOUR** out of **FIVE** questions. Each question carries 20 marks and the maximum mark allocated is **80**. The distribution of the marks for each question is given.
3. Please write all your answers in the Answer Booklet provided.

**QUESTION 1:**

- a. Explain briefly the following **principles of computer security**.
- |                      |                      |
|----------------------|----------------------|
| (i) Confidentiality  | (ii) Integrity       |
| (iii) Authentication | (iv) Non-repudiation |
| (v) Access Control   | (vi) Availability    |
- (6 marks)
- b. Identify the **type of security attack** in the following example and explain your answer.
- (2 marks)
- “The person ‘A’ sends thousands of e-mails per day continuously to a server using a phony return e-mail address.”
- c. **Network Access Security model** is concerned with controlled access to information or resources on a computer system, in the presence of possible opponents. State the **TWO basic tasks** that are needed for this model to cope with unwanted access due to information access threats and service threats.
- (2 marks)
- d. Briefly explain the differences between the following types of **cryptanalysis attacks**, based on ‘what is known to the cryptanalyst’ and the ‘method used’.
- |                               |                               |
|-------------------------------|-------------------------------|
| (i) Ciphertext-only attack    | (ii) Known-plaintext attack   |
| (iii) Chosen-plaintext attack | (iv) Chosen-ciphertext attack |
- (4 marks)
- e. Draw the basic models for **symmetric** and **asymmetric** cryptosystems to provide confidentiality.
- (4 marks)
- f. Answer the following with respect to a group consisting of 15 people and a group leader. Assume the **usage of asymmetric cryptosystem**.
- (2 marks)
- (i) Identify the number of public and private keys needed if all the people in the group wish to send secret messages to each other without involving group leader.
- (ii) Identify the number of public and private keys needed in a scheme, where messages cannot be sent directly between two people and it can be sent only through the group leader.

*Continued...*

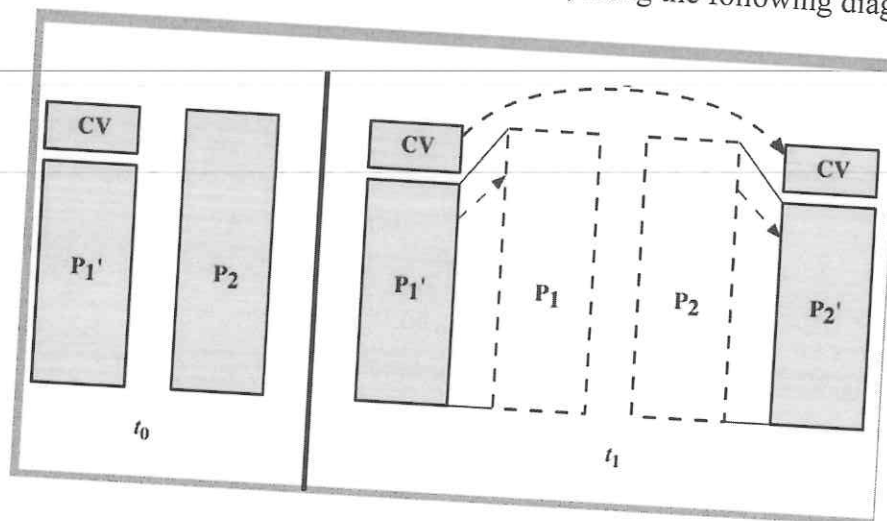
**QUESTION 2:**

a. State the main difference between the following with respect to 'program security'.

- (i) **Computer Viruses and Computer Worms**
- (ii) **Rootkits and Trapdoors**

(2+2=4 marks)

b. Assume that program P1 is infected with the virus cv and when this program is invoked, control is passed to its virus. Briefly explain the steps involved in the **operation of compression virus logic**, which can avoid the detection of the presence of virus based on the length of the code, using the following diagram.



(4 marks)

c. State the **malware countermeasure approaches** that can be used for threat mitigation, if prevention fails.

(2 marks)

d. State what is meant by **SQL injection (SQLi) attack** and give a typical **example**.

(4 marks)

*Continued...*

- e. With reference to database access control, assume that the following convention is followed for **cascading authorization**:

The grant option is used to enable an access right to cascade through a number of users. If a user has an access right with grant option, the user may pass the right to another user. When user 'U' revokes an access right, any cascaded access right is also revoked, unless that access right would exist even if the original grant from 'U' had never occurred. Time of grant is also considered for revoking the access right.

Assume that A, B, and C grant certain privileges on the employee table to X, who in turn grants them to Y, as shown in the following table, with the numerical entries indicating the time of granting.

| User ID | Table    | Grantor | READ | INSERT | DELETE |
|---------|----------|---------|------|--------|--------|
| X       | Employee | A       | 15   | 15     | ---    |
| X       | Employee | B       | 20   | ---    | 20     |
| Y       | Employee | X       | 25   | 25     | 25     |
| X       | Employee | C       | 30   | ---    | 30     |

At time  $t=35$ , B issues the command REVOKE ALL RIGHTS ON Employee FROM X.

Answer the following questions based on the above convention and the given table.

- Which access rights, if any, of Y must be revoked?
- Show the resulting **diagram of access right dependencies**.

(4 marks)

- f. State the main difference between the approaches of **inference detection** during **database design** and **query time**.

(2 marks)

*Continued...*

**QUESTION 3:**

- a. State the **difference** between **Keyless and Keyed Transposition Ciphers** with an example for each. (2 marks)
- b. Assume that plaintext and ciphertext characters are represented as numerical values in  $Z_{26}$  as follows:

|              |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|--------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Plaintext →  | a  | b  | c  | d  | e  | f  | g  | h  | i  | j  | k  | l  | m  | n  | o  | p  | q  | r  | s  | t  | u  | v  | w  | x  | y  | z  |
| Ciphertext → | A  | B  | C  | D  | E  | F  | G  | H  | I  | J  | K  | L  | M  | N  | O  | P  | Q  | R  | S  | T  | U  | V  | W  | X  | Y  | Z  |
| Value →      | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Answer the following questions:

- (i) Assume the usage of **Hill Cipher** and encrypt the following plaintext.

**nation**

Use the following key for encryption.

$$K = \begin{bmatrix} 6 & 3 & 2 \\ 4 & 10 & 6 \\ 3 & 5 & 11 \end{bmatrix}$$

(4 marks)

- (ii) Assume the usage of **Affine Cipher** and assume that the plaintext 'ac' is enciphered to 'DN'.

- Identify the key  $k_1$  to be used with multiplicative cipher and the key  $k_2$  to be used with additive cipher. (2 marks)

- Decrypt** the following ciphertext using affine cipher with the identified keys in modulus 26.

Given ciphertext: **SDS**

(2 marks)

*Continued...*

- c. State the idea behind '**diffusion**' and '**confusion**' properties, which were introduced by Shannon for product cipher. (2 marks)
- d. The design of **Data Encryption Standard (DES)** was revealed by IBM in 1994. One of the criteria for S-box design is given below:

**"If two inputs to an S-box differ in the first two bits (bits 1 and 2) and are the same in the last two bits (5 and 6), the two outputs must be different"**

Test the above criteria by using the pair of inputs, **011100** and **100100** to S-box 1.

**Definition of S-box 1**

|   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 14 | 04 | 13 | 01 | 02 | 15 | 11 | 08 | 03 | 10 | 06 | 12 | 05 | 09 | 00 | 07 |
| 1 | 00 | 15 | 07 | 04 | 14 | 02 | 13 | 10 | 03 | 06 | 12 | 11 | 09 | 05 | 03 | 08 |
| 2 | 04 | 01 | 14 | 08 | 13 | 06 | 02 | 11 | 15 | 12 | 09 | 07 | 03 | 10 | 05 | 00 |
| 3 | 15 | 12 | 08 | 02 | 04 | 09 | 01 | 07 | 05 | 11 | 03 | 14 | 10 | 00 | 06 | 13 |

(4 marks)

- e. With reference to **multiple Data Encryption Standard (DES)**, answer the following:

- (i) State how **encryption and decryption** are done for **Triple DES** using two keys. (2 marks)
- (ii) Briefly explain the following statement for **Double DES**.

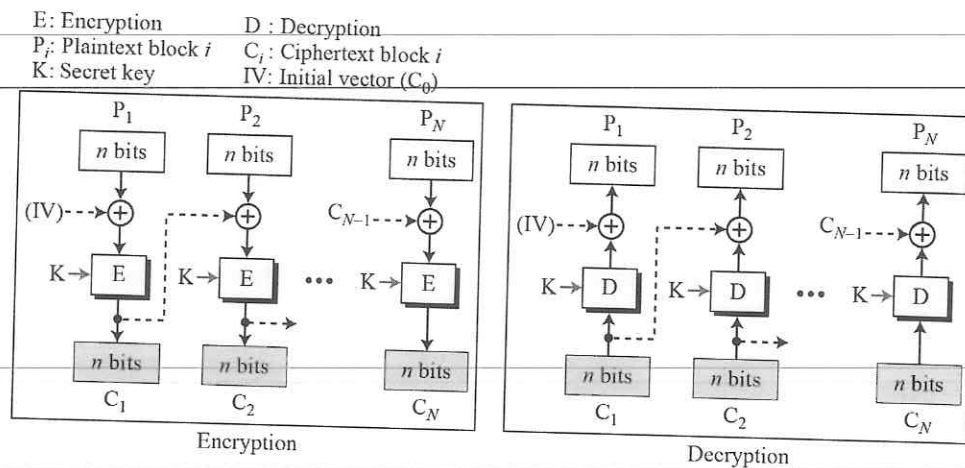
**"Double DES improves the vulnerability of requiring number of tests for key search from  $2^{56}$  in single DES to only  $2^{57}$ , but not to  $2^{112}$ ."**

(2 marks)

*Continued...*

**QUESTION 4:**

- a. With reference to the following diagram that shows the encryption and decryption process for **Cipher Block Chaining (CBC) mode** to be used with modern block ciphers for enciphering text of any size, answer the following:



- (i) Modify the above diagram to show the **encryption and decryption for the last two blocks**, if **ciphertext stealing technique** is used to make the number of bits for ciphertext equal to the plaintext without padding. (4 marks)
- (ii) State the relation between plaintext and ciphertext blocks using **encryption and decryption** equations. (2 marks)
- b. With reference to **Advanced Encryption Standard (AES)**, answer the following:
- (i) Given the plaintext  
 (33 44 55 66 FF EE DD CC BB AA 77 88 99 00 11 22)<sub>H</sub>  
 show the **original contents** of State, displayed as a 4×4 matrix. (1 mark)
- (ii) If  $a$  and  $b$  are two bytes, prove the nonlinearity of the **SubBytes transformation** by performing the following operation.

$$\text{SubBytes}(a \oplus b) \neq \text{SubBytes}(a) \oplus \text{SubBytes}(b)$$

Use SubBytes Transformation table given and the values  
 $a = (0011\ 0110)_2$  and  $b = (1001\ 1100)_2$

(2 marks)

*Continued...*

**Note:****Substitute Bytes Transformation Table (AES S-Boxes)**

|   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |

|   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| B | E7 | CB | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

- (iii) Assume that state before performing ShiftRows transformation on a specific round for AES is given below.

$$\text{State}(\text{beforeShiftRows}) = \begin{bmatrix} FF & EE & DD & CC \\ 00 & 11 & 22 & 33 \\ BB & AA & 99 & 88 \\ 44 & 55 & 66 & 77 \end{bmatrix}$$

Identify the state after performing ShiftRows transformation. (2 marks)

*Continued...*

c. With reference to **Rivest-Shamir-Adleman (RSA)** cryptosystem, answer the following:

- (i) Identify the **public key  $\{e, n\}$**  and **private key  $\{d, n\}$**  for the following data using RSA\_Key\_Generation algorithm given below. **(4 marks)**

$$p=31; q=61; e=23$$

where

$p$  and  $q$  are two prime numbers

$e$  is an integer with  $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$ ;

#### RSA\_Key\_Generation

```
{
  Select two large primes  $p$  and  $q$  such that  $p \neq q$ .
   $n \leftarrow p \times q$ 
   $\phi(n) \leftarrow (p-1) \times (q-1)$ 
  Select  $e$  such that  $1 < e < \phi(n)$  and  $e$  is coprime to  $\phi(n)$ 
   $d \leftarrow e^{-1} \bmod \phi(n)$  //  $d$  is inverse of  $e$  modulo  $\phi(n)$ 
  Public_key  $\leftarrow (e, n)$  // To be announced publicly
  Private_key  $\leftarrow d$  // To be kept secret
  return Public_key and Private_key
}
```

- (ii) With the help of the following algorithms, perform **encryption** using the keys derived in (i) and using the plaintext message **P=3**. **(3 marks)**

**RSA\_Encryption** ( $P, e, n$ ) //  $P$  is the plaintext in  $Z_n$  and  $P < n$

```
{
   $C \leftarrow \text{Fast\_Exponentiation}(P, e, n)$  // Calculation of  $(P^e \bmod n)$ 
  return  $C$ 
}
```

**Square\_and\_Multiply** ( $a, x, n$ )

```
{
   $y \leftarrow 1$ 
  for ( $i \leftarrow 0$  to  $n_b - 1$ ) //  $n_b$  is the number of bits in  $x$ 
  {
    if ( $x_i = 1$ )  $y \leftarrow a \times y \bmod n$  // multiply only if the bit is 1
     $a \leftarrow a^2 \bmod n$  // squaring is not needed in the last iteration
  }
  return  $y$ 
}
```

*Continued...*

- d. With reference to **inv-knapsackSum** algorithm given below, find the elements of  $a$ , which are to be dropped in the knapsack for the following data:

Predefined tuple:  $a = [2 \ 3 \ 6 \ 12 \ 25 \ 50 \ 100 \ 200]$ ;  
Sum of elements in the knapsack,  $s=96$ .

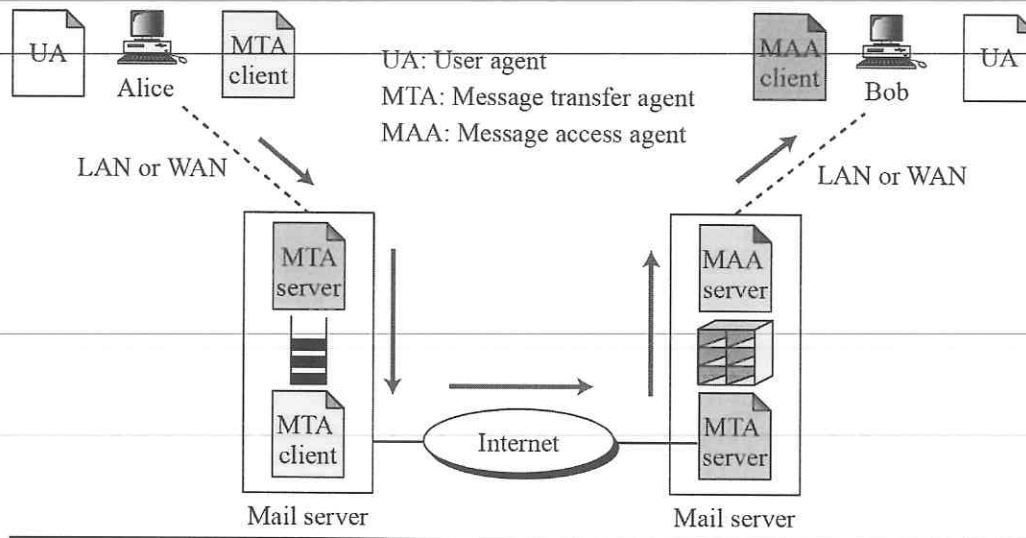
(2 marks)

```
inv_knapsackSum( $s, a[1 \dots k]$ )
{
  for ( $i = k$  down to 1)
  {
    if  $s \geq a_i$ 
    {
       $x_i \leftarrow 1$ 
       $s \leftarrow s - a_i$ 
    }
    else  $x_i \leftarrow 0$ 
  }
  return  $x[1 \dots k]$ 
}
```

*Continued...*

**QUESTION 5:**

- a. With reference to structure of **electronic mail system** as shown in the figure below, answer the following:



- (i) State the steps involved when Alice needs to send a message to Bob. (3 marks)
- (ii) State the **two security services** provided by the content types assuming the usage of **Secure/Multipurpose Internet Mail Extension (S/MIME) protocol** for electronic mail. (1 mark)
- (iii) Assuming the usage of **Radix-64 conversion** method for performing content-Transfer-Encoding in S/MIME protocol, perform the encoding of the following binary data. (4 marks)

10000000 01000010 11111111

Identify the **equivalent codes** based on the following Radix-64 encoding table.

*Continued...*

| Value | Code | Value | Code | Value | Code | Value | Code | Value | Code | Value | Code |
|-------|------|-------|------|-------|------|-------|------|-------|------|-------|------|
| 0     | A    | 11    | L    | 22    | W    | 33    | h    | 44    | s    | 55    | 3    |
| 1     | B    | 12    | M    | 23    | X    | 34    | i    | 45    | t    | 56    | 4    |
| 2     | C    | 13    | N    | 24    | Y    | 35    | j    | 46    | u    | 57    | 5    |
| 3     | D    | 14    | O    | 25    | Z    | 36    | k    | 47    | v    | 58    | 6    |
| 4     | E    | 15    | P    | 26    | a    | 37    | l    | 48    | w    | 59    | 7    |
| 5     | F    | 16    | Q    | 27    | b    | 38    | m    | 49    | x    | 60    | 8    |
| 6     | G    | 17    | R    | 28    | c    | 39    | n    | 50    | y    | 61    | 9    |
| 7     | H    | 18    | S    | 29    | d    | 40    | o    | 51    | z    | 62    | +    |
| 8     | I    | 19    | T    | 30    | e    | 41    | p    | 52    | 0    | 63    | /    |
| 9     | J    | 20    | U    | 31    | f    | 42    | q    | 53    | 1    |       |      |
| 10    | K    | 21    | V    | 32    | g    | 43    | r    | 54    | 2    |       |      |

- b. **Heartbeat protocol** is a sub-protocol in Secure Sockets Layer (SSL)/Transport Layer Security(TLS) Protocol stack, which is typically used to monitor the availability of a protocol entity.
- Briefly explain the **steps** on how the **Heartbeat protocol works** with the help of messages. **(2 marks)**
  - A bug called **Heartbleed** was discovered recently in the widely used openssl implementation of the heartbeat protocol. Briefly explain the **steps** on how this **heartbleed exploit works**. **(2 marks)**
- c. State the main difference between **stateless firewalls** and **stateful firewalls** as a security measure. **(2 marks)**
- d. Briefly explain what do you mean by '**reference monitor**' with respect to operating system security. **(2 marks)**
- e. State the principal difference between the **Bell-Lapadula (BLP)** and **Biba models** of computer security. **(2 marks)**
- f. State any **FOUR techniques** that can be recommended for **wireless network security**. **(2 marks)**

*End of questions*